第27卷 第5期　　工 程 数 学 学 报　　Vol. 27 No. 5
2010年10月　　CHINESE JOURNAL OF ENGINEERING MATHEMATICS　　Oct. 2010

文章编号:1005-3085(2010)05-0865-08

拟 Bent 函数的构造*

张习勇[1]， 郭　华[2]， 滕吉红[2]

(1- 解放军信息工程大学信息工程学院四系，郑州 450002;
2- 北京航空航天大学计算机学院，北京 100083)

摘　要: 拟 Bent 函数在密码系统中可用作非线性组合函数和消息摘要函数，因而具有很好的密码学性质。本文通过计算布尔函数的 Walsh 谱，从映射的角度确定了变元个数不超过六的拟 Bent 函数的代数结构；提出了一般交换群上的扩展组合函数族的概念，研究了这类函数的性质，利用商群给出了扩展组合函数的下降构造，通过组合函数给出了提升构造法，从而得到了一种由扩展组合函数族构造拟 Bent 函数和 Bent 函数的递归构造法，由这种方法可以构造大量拟 Bent 函数和 Bent 函数。另外也构造了几种参数的布尔扩展组合函数。

关键词: 拟 Bent 函数；扩展组合函数族；组合函数族；递归构造

分类号: **AMS**(2000) 94C10; 06E30　　**中图分类号**: TN918.1　　**文献标识码**: A

1　引言和基本定义

在密码学中，人们设计非线性组合函数时考虑的主要准则有：高的代数次数，高的非线性度，满足一定阶的相关免疫性和一定阶数的扩散准则等等。然而，这些准则相互之间有制约关系[1]。针对这种情况，人们相继提出了部分 Bent 函数[2]，半 Bent 函数[3] 等概念，这些函数通过牺牲 Bent 函数的扩散性，来换取满足其它的一些准则。文献 [4] 等提出了 k-阶拟 Bent 函数的概念，它是上述函数的更大类。由于拟 Bent 函数不具有极端的密码学性质，能很好地综合上述密码学准则，因而在这类函数中，较易找到满足上述准则的非线性组合函数。

研究拟 Bent 函数的中心问题包括拟 Bent 函数的性质、构造与应用等。在构造方面，文献 [4] 利用矩阵，研究了拟 Bent 函数的密码学性质，文献 [5] 利用组合函数族给出了拟 Bent 函数的一种递归构造等等。在拟 Bent 函数的结构刻画方面，目前还没有相关的结论。

本文从映射的角度，刻画了六元二阶拟 Bent 函数的代数结构，从而实际上确定了变元个数不超过六的拟 Bent 函数的代数结构。在构造方面，从线性空间和映射的角度，给出了拟 Bent 函数的四种不同构造法。文献 [5] 利用组合函数族 (BF) 给出了拟 Bent 函数的递归构造，但是不能构造 Bent 函数，本文进一步从不同的正交角度提出了扩展组合函数族 (EBF) 的概念，从而结合组合函数族 (BF) 从正交函数组的角度，给出了拟 Bent 函数和 Bent 函数的递归构造。

本文中 G 表示有限 Abel 群，G^* 表示 G 的特征标群，C 表示复数域，$S=\{z\in C\mid |z|=1\}$，ξ_m 表示 m 次本原单位根。对任意的 $f:G\to C$，f 的傅立叶变换定义为

$$\widetilde{f}(\chi)=\sum_{a\in G}f(a)\cdot\chi(a),\quad \forall\,\chi\in G^*.$$

收稿日期: 2008-12-15. **作者简介**: 张习勇 (1975年6月生)，男，博士，副教授. 研究方向：密码学.
***基金项目**: 国家自然科学基金 (60803154).

特别的，布尔函数 f 的傅立叶变换函数称为 f 的Walsh循环谱，记为 $S_{(f)}$。

结合目前许多有关Bent函数的概念，文献[6]定义了一般有限Abel群上的拟Bent函数。

定义1[6] 如果定义在有限Abel群 G 上的函数 $f: G \to S$ 满足

$$|\widetilde{f}(\chi)| = c, \quad 或 \quad |\widetilde{f}(\chi)| = 0, \quad \forall\, \chi \in G^*,$$

其中 c 为实常数，$\mathbf{R}$ 表示实数域。则称 f 是 G 上的拟Bent函数。记 $f^* = \{\chi \in G^* \,|\, \widetilde{f}(\chi) \neq 0\}$，$f^*$ 称为 f 的支撑集。

为给出拟Bent函数的递归构造，文献[5]定义了一族有实际应用背景的拟Bent函数-组合函数族(BF)。下面从不同的正交角度，引入另一族拟Bent函数。

定义2 一个有限Abel群 G 中相对于子群 U 的 (m,t)-扩展组合函数族(EBF)是 G 上的 t 个拟Bent函数，满足对于 G 上的每个特征 $\chi \in G^*$，有：

1) 当 χ 在子群 U 上平凡时，有且只有一个 $|\widetilde{f_j}(\chi)| = m$，其余 $|\widetilde{f_i}(\chi)| = 0$；

2) 当 χ 在子群 U 上非平凡时，所有的 $|\widetilde{f_i}(\chi)| = 0$, $1 \le i \le t$。

特别地，称 $U = \{1_G\}$ 时的EBF为覆盖EBF。

注1 当 $t = 1$, $G = Z_2^n$ 时，EBF就是部分Bent函数[2]。特别地，$t = 1$ 时的覆盖EBF就是 G 上的Bent函数。不难验证：Z_2^n 上的覆盖EBF$\{f_1, \cdots, f_t\}$ 恰好形成 Z_2^n 上的一个Bent互补函数族 $BCFF_t^n(f_i(x))$ (见文献[7])。当对任意的 $i \neq j$, $f_i^* \cap f_j^* = \emptyset$ 时，该命题的逆也成立。拟Bent函数为实值函数，但本文中为方便起见，大多使用的是 p^n 值逻辑函数。

例1 设

$$x \in GF^r(2), \quad y \in GF^{r+k}(2), \quad f(x,y) = \pi(x) \cdot y + \Phi(x),$$

$\Phi(x)$ 为 r 元布尔函数，$i = 1, \cdots, r+k$，若 $\pi(x)$ 是 $GF^r(2)$ 到 $GF^{r+k}(2)$ 的单射，则 $f(x,y)$ 为 $2r + k$ 元 k 阶拟Bent函数。

定义 $GF^{2r+k}(2)$ 上的 $2^t (t \le k)$ 个函数 $h_i\,(x,y) = (-1)^{f_i(x,y)}$，其中

$$f_i(x,y) = \pi_i(x) \cdot y + \Phi_i(x),$$

$\pi_i(x)$ 为 $GF^r(2)$ 到 $GF^{r+k}(2)$ 的单射，$1 \le i \le 2^t$。记

$$E_i = \big\{\pi_i(x) : x \in GF^r(2)\big\}, \quad F = \bigcup_{1 \le i \le 2^t} E_i,$$

若满足对任意的 $i \neq j$, $E_i \cap E_j = \emptyset$，且 F 恰好是 $GF^{r+k}(2)$ 中的一个 $GF(2)$ 上的 $r+t-1$ 维子空间，则 $\{h_i \,|\, 1 \le i \le 2^t\}$ 构成 $GF^{2r+k}(2)$ 上相对于二阶子群的 $(2^{r+k}, 2^t)$−EBF。

2 六元布尔拟Bent函数的代数结构

引理1 不存在三元布尔函数 $f(x)\,(x = (x_0, x_1, x_2) \in GF^3(2))$，使得对于任意的仿射函数 $\phi(x)$，$f(x) + \phi(x)$ 都是平衡函数。

证明 可证得在线形等价的意义下，$f(x)$ 具有代数形式 $\phi_1(x)$, $x_0x_1 + \phi_1(x)$，或 $x_0x_1x_2 + \phi_1(x)$，其中 $\phi_1(x)$ 为仿射函数。这样对于任意的仿射函数 $\phi(x)$，$f(x)+\phi(x)$ 都不是平衡函数。

引理2 若布尔函数 $f(x_0, x_1, x_2)$ 的重量为2或6，则在线性等价的意义下，$f = x_0x_1$。

证明 当 $f(x_0, x_1, x_2)$ 的重量为2时，设 $f(a_0, a_1, a_2) = 1$, $f(b_0, b_1, b_2) = 1$，而在 $GF^3(2)$ 的其余6点上 f 取值为0。这样

$$\begin{aligned} f(x_0, x_1, x_2) \;=\; & (x_0 + a_0 + 1)(x_1 + a_1 + 1)(x_2 + a_2 + 1) \\ & +(x_0 + b_0 + 1)(x_1 + b_1 + 1)(x_2 + b_2 + 1), \end{aligned}$$

对该式做线性变换，即可得证。

对于重量为 6 的情况，可类似证明。

引理 3[8] 任一个次数为 3 的六元布尔函数均具有代数形式

$$f(x,y)=x_0x_1x_2+x_0h_0(y)+x_1h_1(y)+x_2h_2(y)+g(y),$$

其中 h_0, h_1, h_2, g 均为三元布尔函数，且 h_0, h_1, h_2 代数次数不超过 2。

引理 4 设六元布尔函数

$$f_1(x,y)=x_0h_0(y)+x_1h_1(y)+x_2h_2(y)+g(y)=x\cdot\pi(y)+g(y),$$

$$f(x,y)=x_0x_1x_2+f_1(x,y),$$

其中

$$x=(x_0,x_1,x_2),\quad y=(y_0,y_1,y_2)\in GF^3(2).$$

设 $h_0(y)+h_1(y)+h_2(y)+g(y)$ 为仿射函数，且 $k_w=|\{y\,|\,\pi(y)=w\}|$。则 $f(x,y)$ 为六元二阶拟 Bent 函数，当且仅当 $k_w=0,2,4$，且当 $k_w=4$ 时，$\{y\,|\,\pi(y)=w\}$ 不是 $GF^3(2)$ 的线性子空间或其平移。

证明 记

$$E=\big\{(x,y)\in GF^6(2)\,|\,x_0=x_1=x_2=1\big\},\quad f_2(y)=h_0(y)+h_1(y)+h_2(y)+g(y),$$

对于任意的 w, $v\in GF^3(2)$，有

$$\begin{aligned}S_{(f)}(w,v)&=\sum_{(x,y)\in E}(-1)^{f(x,y)+wx+vy}+\sum_{(x,y)\in G\setminus E}(-1)^{f(x,y)+wx+vy}\\&=\sum_{(x,y)\in G}(-1)^{f_1(x,y)+wx+vy}-2\sum_{y\in E}(-1)^{f_2+vy+w_0+w_1+w_2}\\&=S_1(w,v)-2S_2(w,v).\end{aligned}$$

上式中

$$S_1(w,v)=\sum_{(x,y)\in G}(-1)^{f_1(x,y)+wx+vy},\quad S_2(w,v)=\sum_{y\in E}(-1)^{f_2+vy+w_0+w_1+w_2}.$$

进一步的有

$$S_1(w,v)=\sum_{(x,y)\in G}(-1)^{f_1(x,y)+wx+vy}=\sum_{y\in GF^3(2)}(-1)^{g(y)+vy}\sum_{x\in GF^3(2)}(-1)^{(\pi(y)+w)x}.$$

不妨设仿射函数 $f_2(y)=0$，这样

$$g(y)=h_0(y)+h_1(y)+h_2(y),$$

从而当 $\pi(y)=w=(w_0,w_1,w_2)$ 时，$g(y)=w_0+w_1+w_2$。故

$$\begin{aligned}S_{(f)}(w,v)&=S_1(w,v)-2S_2(w,v)\\&=(-1)^{w_0+w_1+w_2}\Big(\sum_y(-1)^{vy}\sum_x(-1)^{(\pi(y)+w)x}-2\sum_y(-1)^{vy}\Big)\\&=8\cdot(-1)^{w_0+w_1+w_2}\Big(\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)\Big).\end{aligned}$$

上式中 $\delta_0(v)$ 表示特征函数，即当 $v=0$ 时，$\delta_0(v)=1$，否则 $\delta_0(v)=0$。

(必要性) 当 $f(x,y)$ 为6元2阶拟Bent函数时，对于任意的 $w,\ v\in GF^3(2)$，$S_{(f)}(w,v)=0,\ \pm16$，这样上式中

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=0,\ \pm2,$$

从而 $k_w=0,2,4$。否则当 $k_w=1,3,5,6,7,8$ 时，取 $v=0$，有

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=-1,1,3,4,5,6,$$

矛盾。当 $k_w=4$ 时，设 $\pi^{-1}(w)=\{y_1,y_2,y_3,y_4\}$，若 $\{y_1,y_2,y_3,y_4\}$ 是 $GF^3(2)$ 的线性子空间或其平移，则存在 $v\neq0$，使得

$$(-1)^{vy_1}+(-1)^{vy_2}+(-1)^{vy_3}+(-1)^{vy_4}=\pm4,$$

从而

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=\pm4,$$

矛盾。

(充分性) 只需说明

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=0,\pm2$$

即可。

当 $k_w=0$ 时

$$\sum_{\pi(y)=w}(-1)^{vy}=0,$$

所以

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=0,\ -2.$$

当 $k_w=2$ 时，设 $\pi^{-1}(w)=\{y_1,y_2\}$，则

$$\sum_{\pi(y)=w}(-1)^{vy}=(-1)^{vy_1}+(-1)^{vy_2}.$$

若 $v=0$，$(-1)^{vy_1}+(-1)^{vy_2}=2$，$\delta_0(v)=1$，从而

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=0.$$

当 $v\neq0$ 时，$(-1)^{vy_1}+(-1)^{vy_2}=0,\pm2$，$\delta_0(v)=0$，从而

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=0,\pm2.$$

当 $k_w=4$ 时，设 $\pi^{-1}(w)=\{y_1,y_2,y_3,y_4\}$，则

$$\sum_{\pi(y)=w}(-1)^{vy}=(-1)^{vy_1}+(-1)^{vy_2}+(-1)^{vy_3}+(-1)^{vy_4}.$$

若 $v=0$，$(-1)^{vy_1}+(-1)^{vy_2}+(-1)^{vy_3}+(-1)^{vy_4}=4$，$\delta_0(v)=1$，从而

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=2.$$

若 $v\neq 0$，不难验证，当 $\{y_1,y_2,y_3,y_4\}$ 不是 $GF^3(2)$ 的线性子空间或其平移时，$(-1)^{vy_1}+(-1)^{vy_2}+(-1)^{vy_3}+(-1)^{vy_4}=0,\pm 2$，而 $\delta_0(v)=0$，从而

$$\sum_{\pi(y)=w}(-1)^{vy}-2\delta_0(v)=0,\pm 2.$$

定理1　次数为3的函数 $f(x,y)\,(x=(x_0,x_1,x_2),\ y=(y_0,y_1,y_2)\in GF^3(2))$ 为六元二阶拟 Bent 函数，当且仅当在等价意义下，$f(x,y)$ 具有形式 $x_0x_1x_2+x_0h_0(y)+x_1h_1(y)+x_2h_2(y)+g(y)$，其中 h_0,h_1,h_2,g 均为三元布尔函数，h_0,h_1,h_2 代数次数不超过2，且满足：

1)　$GF^3(2)$ 上的映射 $\pi:(y_0,y_1,y_2)\longrightarrow(h_0(y),h_1(y),h_2(y))$ 满足

$$k_w=\big|\{y\,|\,\pi(y)=w\}\big|=0,2,4,\quad \forall\, w\in GF^3(2),$$

且当 $k_w=4$ 时，$\{y\,|\,\pi(y)=w\}$ 不是 $GF^3(2)$ 的线性子空间或其平移。

2)　三元函数 $f_2=h_0+h_1+h_2+g$ 为仿射函数。

证明 (必要性)　当 $f(x,y)$ 代数次数为3时，由引理3可知 $f(x,y)$ 具有形式 $x_0x_1x_2+x_0h_0(y)+x_1h_1(y)+x_2h_2(y)+g(y)$，其中 h_0,h_1,h_2,g 如题所设。又记 $f_1(x,y)=x_0h_0(y)+x_1h_1(y)+x_2h_2(y)+g(y)$。沿用引理4的符号，有

$$S_{(f)}(w,v)=S_1(w,v)-2S_2(w,v),\quad \forall\, w,v\in GF^3(2).$$

由 $f(x,y)$ 为6元2阶拟 Bent 函数知，对于任意的 $w,v\in GF^3(2)$，$S_{(f)}(w,v)=0,\pm 16$，不难看出 $S_1(w,v)\equiv 0\,(\mathrm{mod}\,8)$，从而 $S_2(w,v)\equiv 0\,(\mathrm{mod}\,4)$。

假设三元函数 $f_2=h_0+h_1+h_2+g$ 不是仿射函数，则必有 $S_2(w,v)=0$ 或 ± 4。若对于任意的 $v\in GF^3(2)$，$f_2+v\cdot y$ 为平衡函数，由引理1知这是不可能的。

所以存在 $v\in GF^3(2)$，使得 $f_2+v\cdot y$ 的重量为2或6。由引理2，不妨设 $f_2=y_0y_1$。

这样在全部八个函数 $h_v=h_0+h_1+h_2+g+vy\,(v\in GF^3(2))$ 中，有四个为平衡函数，另外四个函数的重量为2或6。相对应若取定 w，则四个 $S_2(w,v)=0$，另四个 $S_2(w,v)=\pm 4$。

若存在 $u\in GF^3(2)$，使得 $k_u=0$，此时 $S_1(u,v)=0$。取 v，使得 $S_2(u,v)=\pm 4$。这样 $S_{(f)}(u,v)=S_1(u,v)-2S_2(u,v)=\pm 8$，与 $f(x,y)$ 为6元2阶拟 Bent 函数相矛盾。

若存在 $u'\in GF^3(2)$，使得 $k_{u'}=1$，此时 $S_1(u',v)=\pm 8$。取 v，使得 $S_2(u',v)=0$。这样 $S_{(f)}(u',v)=S_1(u',v)-2S_2(u',v)=\pm 8$，也与 $f(x,y)$ 为六元二阶拟 Bent 函数相矛盾。

易知

$$\sum_{w\in GF^3(2)}k_w=8,$$

且 $k_w\geq 0$。但 $k_w\neq 0,1$，矛盾。

综上可知假设不成立，也即函数 $h_0+h_1+h_2+g$ 必是仿射函数。

当函数 $h_0+h_1+h_2+g$ 为仿射函数时，由引理4可知，对任意的 $w\in GF^3(2)$，$k_w=0,2,4$，且当 $k_w=4$ 时，$\{y\,|\,\pi(y)=w\}$ 不是 $GF^3(2)$ 的线性子空间或其平移。

(充分性)　即引理4。

注2 由文献[4]可知，n元k阶拟Bent函数的代数次数不超过$(n-k)/2+1$，这样六元四阶、五元三阶拟Bent函数均为二次型，其代数标准型为一个低元Bent函数和一个仿射函数之和，就其本质而言与二元或四元Bent函数等价。又类似定理1，可刻画代数次数为3的五元一阶拟Bent函数的结构，从而对于变元个数不超过6的拟Bent函数，其结构实际可完全确定。

3 拟Bent函数和Bent函数的递归构造

第一节定义了一类特殊的拟Bent函数族：扩展组合函数族(EBF)，本节则给出EBF的几种构造法，并结合组合函数族(BF)，给出一种Bent函数和拟Bent函数的递归构造。

下面的EBF提升构造法是较显然的。

定理2 设有限加法Abel群$M\subseteq G$，$|G/M|=s$，$s\,|\,t$，M上存在相对于子群U的(m,t)-EBF$\{f_i\,|\,1\le i\le t\}$，设商群$G/M=\{y_1+M,\cdots,y_s+M\}$，定义$G$上的函数：对任意的$x\in G$，$h_j(x)=f_{i+(j-1)s}(z)$，若$x\equiv y_i\,(\mathrm{mod}M)$，其中$x=y_i+z$，$z\in M$，$1\le i\le s$，$1\le j\le t/s$。则$\{h_1(x),\cdots,h_{t/s}(x)\}$是$G$上相对于$U$的$(m,t/s)$-EBF。

下面的几个结论给出了另外几种构造。

引理5 设有限加法Abel群G/U上存在参数为(m,t)的覆盖EBF$\{f_i\,|\,1\le i\le t\}$，其中$|U|=u$，则G上存在参数为(um,t)的相对于子群U的EBF。

证明 设π表示自然同态：$G\to G/U$，为方便，记$\pi(x)=\bar{x}$，下文同。定义G上的函数对任意的$x\in G$，$h_i(x)=f_i(\bar{x})$，由定义2不难验证函数组$\{h_1,\cdots,h_t\}$即为所求。

定理3 设有限加法Abel群G/U上存在参数为(m,t)的覆盖EBF，同时G上存在参数为(um,s)的相对于子群U的BF$\{h_i\,|\,1\le i\le s\}$，则G上存在参数为$(um,t+s)$的覆盖EBF。

证明 由引理5可知，当G/U上存在参数为(m,t)的覆盖EBF时，则G中存在参数为(um,t)的相对于子群U的EBF$\{f_i\,|\,1\le i\le t\}$。由定义2可验证$\{f_i\,|\,1\le i\le t\}\cup\{h_i\,|\,1\le i\le s\}$是$G$上参数为$(um,t+s)$的覆盖EBF。

引理5说明了商群上的覆盖EBF与大群上的EBF之间的关系，实际上这是一种等价关系。

引理6 设$\{f_i\,|\,1\le i\le t\}$是有限加法Abel群G上参数为(m,t)的相对于子群U的EBF，对任意的$x_1,x_2\in G$，若满足$x_1\equiv x_2(\mathrm{mod}\,U)$，则对任意的$i$，有$f_i(x_1)=f_i(x_2)$。

证明 由熟知的反演公式以及EBF的定义可知

$$|G|\cdot f_i(x_1)=\sum_{\chi\in G^*}\widetilde{f}_i(\chi)\cdot\overline{\chi(x_1)}=\sum_{\chi\in N^{\perp}}\widetilde{f}_i(\chi)\cdot\overline{\chi(x_1)}\,.$$

由于$x_1\equiv x_2(\mathrm{mod}\,U)$，当$\chi\in U^{\perp}$时，$\chi(x_1)=\chi(x_2)$，于是

$$\sum_{\chi\in N^{\perp}}\widetilde{f}_i(\chi)\cdot\overline{\chi(x_1)}=\sum_{\chi\in N^{\perp}}\widetilde{f}_i(\chi)\cdot\overline{\chi(x_2)}=\sum_{\chi\in G^*}\widetilde{f}_i(\chi)\cdot\overline{\chi(x_2)}=|G|\cdot f_i(x_2)\,,$$

从而有$f_i(x_1)=f_i(x_2)$。

定理4 有限加法Abel群G上存在相对于子群U的(m,t)-EBF$\{f_i\,|\,1\le i\le t\}$，当且仅当商群G/U上存在$(m/u,t)$-覆盖EBF$\{h_i\,|\,1\le i\le t\}$，使得$f_i(x)=h_i(\bar{x})$，其中$|U|=u$。

证明(必要性) 由引理6可知对任意的$x_1,x_2\in G$，当$x_1\equiv x_2(\mathrm{mod}\,U)$时，有$f_i(x_1)=f_i(x_2)\,(1\le i\le t)$。这样就可定义$G/U$上的函数$h_i$:对任意的$\bar{x}\in G/U$，令$h_i(\bar{x})=f_i(x)$。

可验证函数组$\{h_i\,|\,1\le i\le t\}$是G/U上参数为(m,t)的覆盖EBF。

(充分性) 即引理5。

注 3 当 G 取为初等 2-群，且 $\{-1/2\cdot f_i+1/2\,|\,1\le i\le t\}$ 都是布尔函数时，上述结论可看成是文献 [2] 中 Bent 函数和部分 Bent 函数关系的推广。当 $t=1$ 时，上述结论就是文献 [6] 中的定理 4。

定理 2、3、4 实际上给出了由小群中的 EBF 和 BF 递归构造大群上的 EBF 或 Bent 函数的递归算法，在本文的最后，仅以布尔函数为例，给出具体应用。

引理 7 若 $l\ge 2$, $t\ge 1$，则群

$$G_{l,t}=Z_2^{2l+t-2}$$

中存在相对于任意二阶子群 U 的 $(2^{l+t-1},2^{t-1})$-BF。

证明 设

$$x=(x_1,\cdots,x_{l-1}),\quad y=(y_1,\cdots,y_{l+t-1}),\quad f_i(x,y)=\pi_i(x)\cdot y+\Phi_i(x),\quad i=1,\cdots,2t-1,$$

其中 $\Phi_i(x)$ 为 r 元布尔函数，$\pi_i(x)$ 为 $GF^{l-1}(2)$ 到 $GF^{l+t-1}(2)$ 的单射，则 $f_i(x,y)$ 为 $2l+t$-2 元 t 阶拟 Bent 函数。

$$E_i=\{\pi(x):x\in GF^{l-1}(2)\},\quad F=\bigcup_{1\le i\le 2^{t-1}}E_i,$$

若满足对任意的 $i\neq j$，$E_i\cap E_j=\varnothing$，且 $GF^{l-1+t}(2)\setminus F$ 是 $GF^{l-1+t}(2)$ 中的一个 $GF(2)$ 上的 $l+t-2$ 维子空间，则可验证 $\{f_i\,|\,1\le i\le 2^{t-1}\}$ 构成 $GF^{2l+t-2}(2)$ 上相对于二阶子群的 $(2^{l+t-1},2^{t-1})$-BF。

定理 5 设 $G_{l,t}=Z_2^{2l+t-2}$，且 $l\ge 2$, $t\ge m\le 0$，则 $G_{l,t+m}$ 中存在参数为 $(2^{l+t-1},2^{t-m})$ 的覆盖 EBF。

证明 先不妨设 $m=0$，对 t 使用归纳法。$t=0$ 时，$G_{l,0}$ 中参数为 $(2^{l-1},1)$ 的覆盖 EBF 就是 Z_2^{2l-2} 中的 Bent 函数，自然是存在的。

假设命题对于 $t-1$ 时是成立的，即 $G_{l,t-1}$ 中存在参数为 $(2^{l+t-2},2^{t-1})$ 的覆盖 EBF $\{g_i\,|\,1\le i\le 2^{t-1}\}$。由引理 5 知，在 $G_{l,t}$ 中存在相对于任意二阶子群 U 的

$$(2^{l+t-1},2^{t-1})\text{-EBF}\,\{h_i(x)=g_i(\bar{x})\,|\,1\le i\le 2^{t-1}\}.$$

又由引理 7，在 $G_{l,t}$ 中存在相对于 U 的 $(2^{l+t-1},2^{t-1})$-BF$\{f_i\,|\,1\le i\le 2^{t-1}\}$。

从而 $\{f_i,h_i\,|\,1\le i\le 2^{t-1}\}$ 为 $G_{l,t}$ 中参数为 $(2^{l+t-1},2^t)$ 的覆盖 EBF (定理 3)，故命题对于 t 时也是成立的。由归纳法可知对于一般的 $t\ge 0$, $m=0$，命题成立。

当 $m\ge 1$ 时，设 φ 为集合 $\{1,\cdots,2^m\}$ 到 Z_2^m 上的双射，且

$$\varphi(i)=\big(a_{i(2l+t-1)},\cdots,a_{i(2l+t+m-2)}\big).$$

若 $\{f_i\,|\,1\le i\le 2^t\}$ 为 $G_{l,t}$ 中的 $(2^{l+t-1},2^t)$-覆盖 EBF，由定理 2，对于 $1\le j\le 2^{t-m}$，函数组

$$f_j(x_1,\cdots,x_{2l+t+m-2})=\sum_{1\le i\le 2^m}\Bigg(\prod_{k=2l+t-1}^{k=2l+t+m-2}(x_k+a_{ik})\Bigg)\cdot f_{i+(j-1)2^m}(x_1,\cdots,x_{2l+t-2})$$

是 $Z_2^{2l+t+m-2}$ 中参数为 $(2^{l+t-1},2^{t-m})$ 的覆盖 EBF。特别地，$t=m$ 时，即可得到 Bent 函数。

注 4 由注 1 知，群 Z_2^n 上的覆盖 EBF 不仅是拟 Bent 函数族，又是 Bent 互补函数族，故定理 5 不但给出了拟 Bent 函数、EBF 和 Bent 函数的递归构造算法，也从递归的角度给出了 Bent 互补函数族的一种构造方法，而后者在密码学和通信领域中也具有广泛应用。

参考文献：

[1] 冯登国，裴定一. 密码学导引[M]. 北京：科学出版社，1999
Feng D G, Pei D Y. Cryptography[M]. Beijing: Science Press, 1999

[2] 滕吉红等. 一类 k 阶拟 Bent 函数密码性质的矩阵特征[J]. 计算机学报，2004, 27(4): 543-547
Teng J H, *et al. The matrix characteristics of the cryptographic properties of a special kind of k-order* quasi-Bent functions[J]. Chinese Journal of Computers, 2004, 27(4): 543-547

[3] 胡磊，裴定一，冯登国. 一类 Bent 函数的构造[J]. 中国科学院研究生院学报，2002, 19(2): 103-106
Hu L, Pei D Y, Feng D G. Construction of a class of Bent functions[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2002, 19(2): 103-106

[4] 赵亚群. 部分 Bent 函数和广义部分 Bent 函数的性质及构造[D]. 郑州信息工程大学博士论文，2000
Zhao Y Q. Some properties and constructions of partial Bent functions and generalized partial Bent functions[D]. Thesis of Zhengzhou University of Information and Engineering, 2000

[5] 张习勇，韩文报. 一种拟 Bent 函数的构造方法[J]. 工程数学学报，2004, 21(6): 118-122
Zhang X Y, Han W B. A construction of quasi-Bent functions[J]. Chinese Journal of Engineering Mathematics, 2004, 21(6): 118-122

[6] 张习勇，韩文报. 拟 Bent 函数的性质和构造[J]. 数学学报，2004, 47(6): 1175-1184
Zhang X Y, Han W B. Some properties and constructions of quasi-Bent functions[J]. Acta Mathematica Sinica, 2004, 47(6): 1175-1184

[7] 许成谦，杨义先，胡正名. Bent 互补函数族的性质和构造[J]. 电子学报，1997, 25(10): 52-56
Xu C Q, Yang Y X, Hu Z M. The properties and constrution methods of families of Bent complementary functions[J]. Chinese Journal of Acta Electronica Sinica, 1997, 25(10): 52-56

[8] Carlet C. Two new classes of Bent functions[C]// Advances in Cryptology-EURCRYPT'93, Lofthus: Springer-Verlag, 1994: 77-101

Constructions of Quasi-Bent Functions

ZHANG Xi-yong[1], GUO Hua[2], TENG Ji-hong[2]

(1- Zhengzhou Information Science and Technology Institute, PO Box 1001-745, Zhengzhou 450002;
2- School of Computer Science & Engineering, Beihang University, Beijing 100083)

Abstract: Qausi-Bent functions have good cryptographic properties and are employed as nonlinear combining functions and Hash functions in cryptography. In this paper, we firstly characterize the structures of quasi-Bent functions with variables not exceeding 6 by calculating Walsh spectrum of Boolean functions. We also introduce the concept of extended building functions (EBFs) in general finite Abelian groups and give some properties of this kind of functions. Using quotient group and the concept of building functions, we present a descending construction and a lifting construction, respectively. Thus we obtain a recursive construction of quasi-Bent functions and Bent functions by using the tool of EBFs. A great deal of quasi-Bent functions and Bent functions can thus be constructed. Using above methods, we give extended Boolean building functions with some parameters.

Keywords: quasi-Bent function; extending building function; building functions; recursion construction

Received: 15 Dec 2008. **Accepted:** 15 July 2009.
Foundation item: The National Natural Science Foundation of China (60803154).